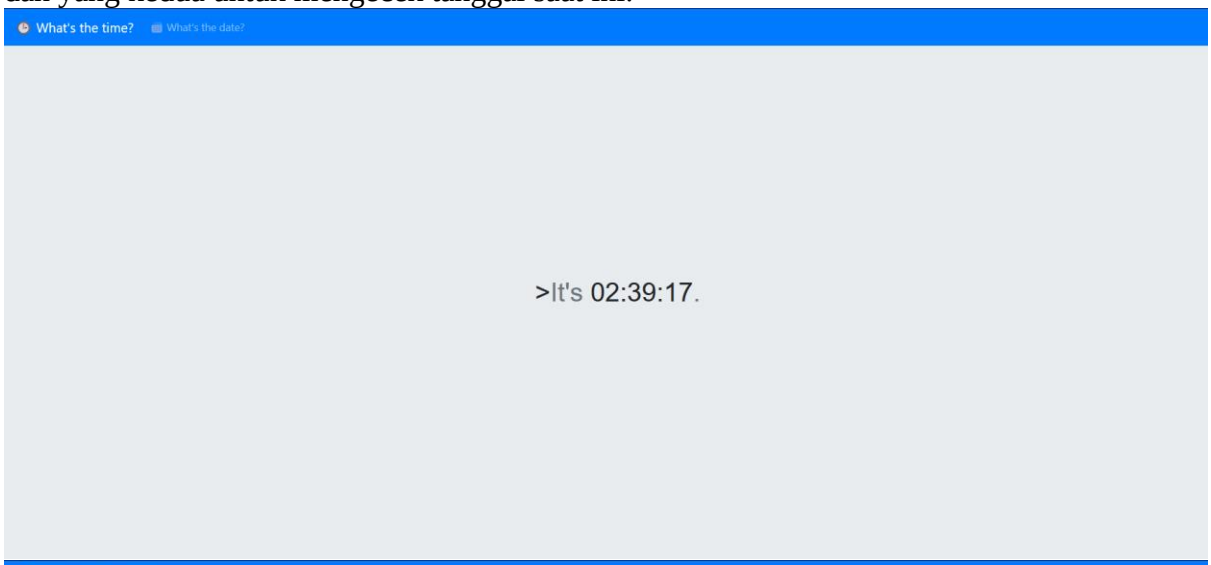
CHALLENGE NAME

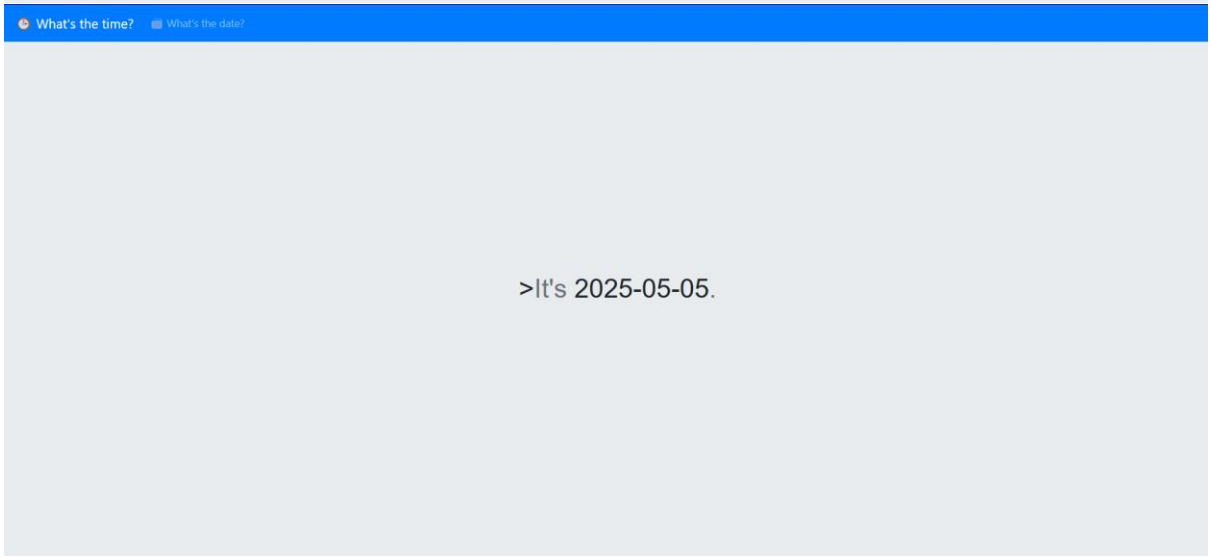
TimeKORP
Are you ready to unravel the mysteries and expose the truth hidden within KROP's digital domain? Join the challenge and prove your prowess in the world of cybersecurity. Remember, time is money, but in this case, the rewards may be far greater than you imagine.

Scenario File

IDENTIFYING

Ini adalah tampilan awal pada aplikasi web ketika diakses, setelah melakukan pengecekkan pada fitur, saya menemukan bahwa ada dua fitur, yang pertama untuk mengecek jam saat ini dan yang kedua untuk mengecek tanggal saat ini.



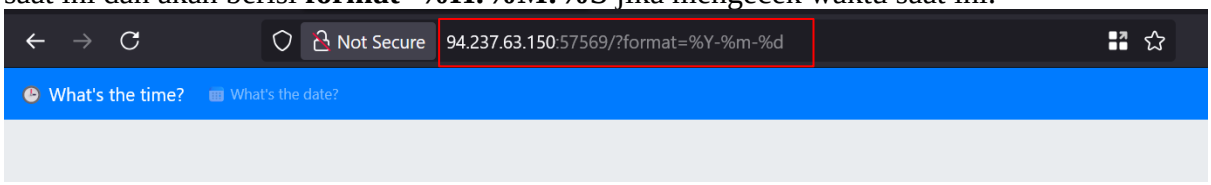


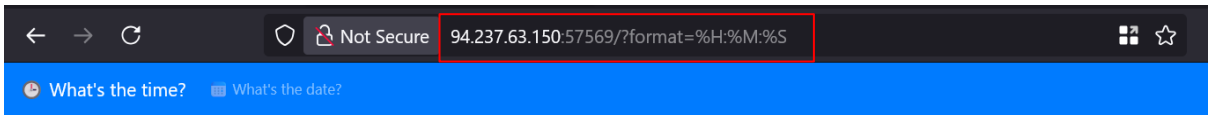
Selanjutnya saya mencoba mengidentifikasi *scenario file* yang diberikan pada tantangan ini. Pada ***file TimeModel.php*** saya menemukan sebuah kode yang menarik perhatian saya, yaitu aplikasi web menggunakan *function* **exec()** untuk menjalankan perintah **date** yang digunakan untuk mendapatkan waktu atau tanggal saat ini, *function* ini rentan terhadap serangan ***Command Injection***.

```php
<?php
class TimeModel
{
    public function __construct($format)
    {
        $this->command = "date '+" . $format . "' 2>&1";
    }

    public function getTime()
    {
        $time = exec($this->command);
        $res  = isset($time) ? $time : '?';
        return $res;
    }
}
```

Variable **$format** akan berisi nilai parameter **format=%Y-%m-%d** untuk mengecek tanggal saat ini dan akan berisi **format=%H:%M:%S** jika mengecek waktu saat ini.





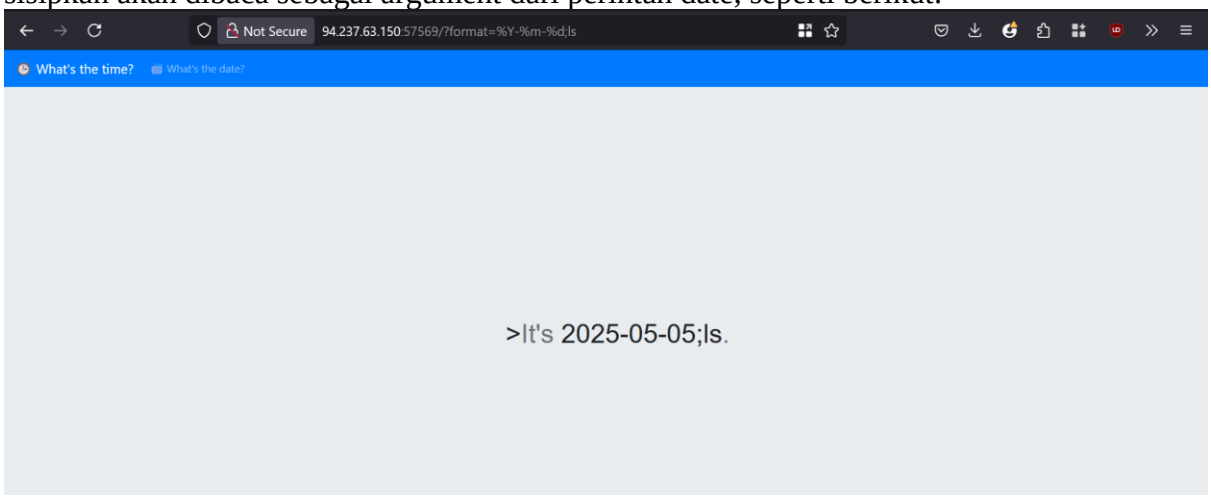
Jika pada sistem operasi Linux, perintah ini akan menjadi seperti berikut:

Date

Time

EXPLOITING

Karena terdapat tanda petik satu sebelum symbol (+) dan sebelum **2>&1** perintah yang kita sisipkan akan dibaca sebagai argument dari perintah date, seperti berikut:



Seperti yang lihat, saya menambahkan **;ls** sesudah **%Y-%m-%d**, tetapi perintah yang kita masukkan hanya akan dibaca sebagai argument perintah **date**. Untuk mengatasi hal ini kita perlu menambahkan tanda petik satu diantara payload yang kita tambahkan seperti berikut:

Sebelum:

```
"date '+%Y-%m-%d;ls' 2>&1"
```

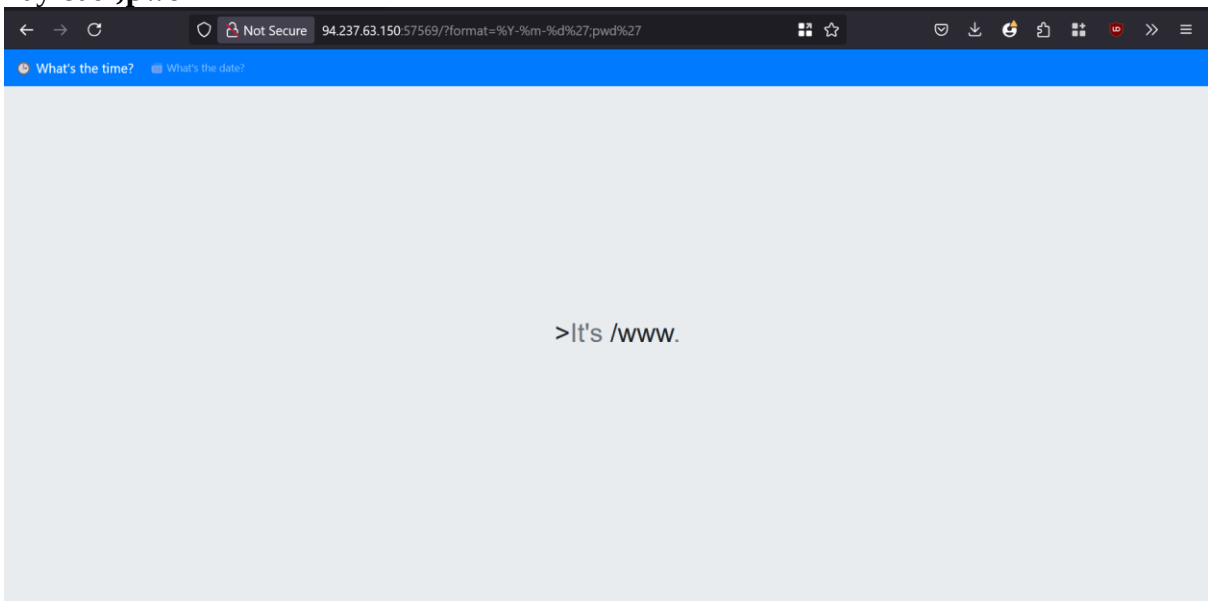
Sesudah:

```
"date '+%Y-%m-%d';ls'' 2>&1"
```

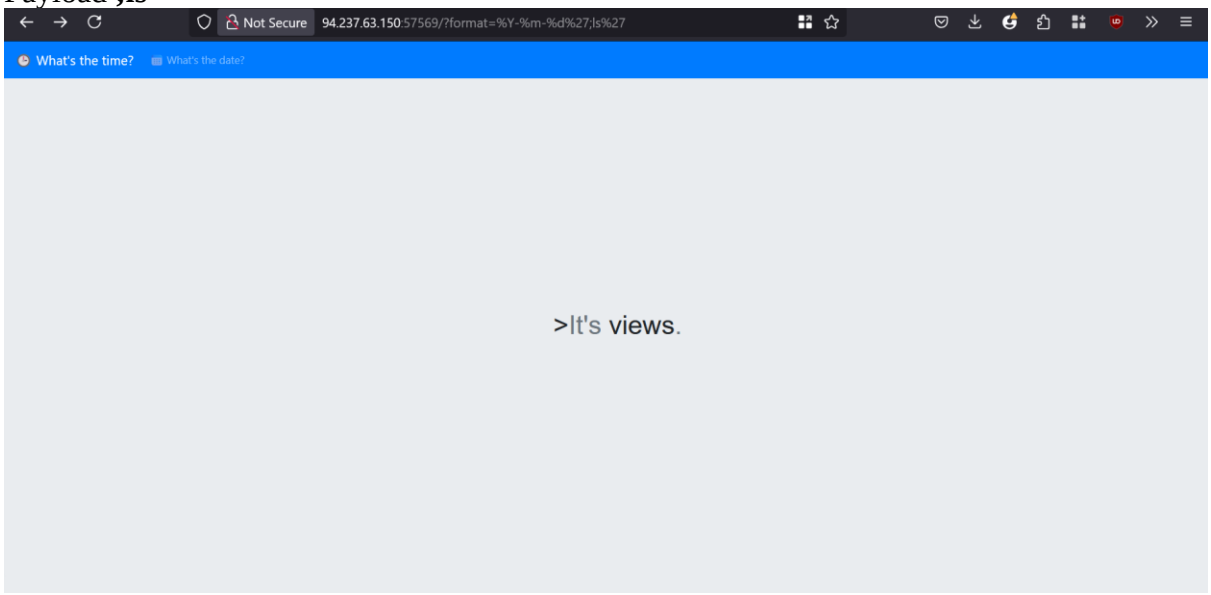
Jadi, **+%Y-%m-%d** sudah dibungkus oleh tanda petik satu dan tanda petik sisa sebelum **2>&1** menjadi sebuah string kosong. Payload yang kita masukkan tidak akan dibaca sebagai argument dari perintah **date** lagi oleh *function* **exec()**.

Seperti yang terlihat, saya berhasil melakukan serangan *Command Injection*. Selanjutnya saya perlu mengecek pada direktori mana saya berada.

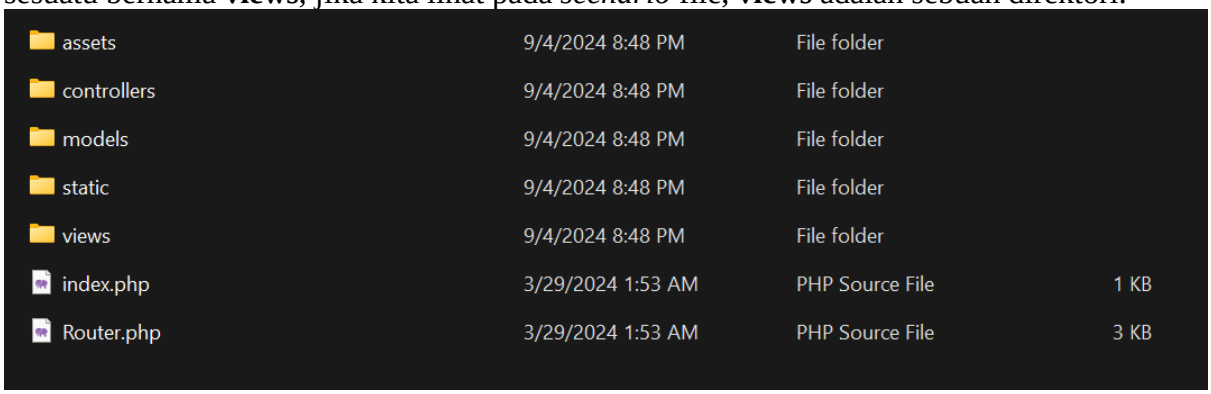
Payload **;pwd**



Payload **;ls**



Seperti yang terlihat saya berada pada direktori **/www** dan pada direktori tersebut terdapat sesuatu bernama **views**, jika kita lihat pada *scenario* file, **views** adalah sebuah direktori.



Lalu flag berada pada direktori satu tingkat di atas dari direktori **/www**, berarti untuk membaca flag kita perlu menggunakan payload **cat ../flag**.

Seperti yang terlihat, saya berhasil mendapatkan flagnya:
HTB{t1m3_f0r_th3_ult1m4t3_pwn4g3_9b46dbadf43511ab8e26381b5c6edf68}